Abstract

IT security is facing expanding challenges in the age of digitalization, but many organizations are still not prepared for the increased regulation level and threat landscape. This white paper covers the definition of critical infrastructure across countries and discusses the importance of taking a holistic approach in the development and deployment of an effective IT security strategy. The paper provides an overview of the current situation regarding cyberattacks, discusses the various types of cyber threats, and the potential consequences of an inadequate IT security strategy. It also provides details on the increasing global regulation level by countries and consequently, the needs for critical infrastructure industries to adopt the specific steps to implement such a strategy.
## Contents

1 ABOUT THE TÜV SÜD EXPERT ........................................................................ 3

2 INTRODUCTION .......................................................................................... 4

2 THE GROWING IT SECURITY THREAT AND ITS CONSEQUENCES ............... 5

3 IT SECURITY REGULATIONS ....................................................................... 8

4 TYPES OF IT SECURITY THREATS AND VULNERABILITIES ....................... 11

5 ELEMENTS FOR BROADER APPROACH TO IT SECURITY .......................... 12

6 STEP TOWARDS AN EFFECTIVE IT SECURITY STRATEGY ......................... 13

7 HOW CAN TÜV SÜD HELP YOU? ............................................................... 14
About the TÜV SÜD expert

Francisco Baraona  
Head of Global Enterprise IT Security, TÜV SÜD Management Service  
Francisco Baraona is heading the global enterprise IT security department within TÜV SÜD Management Service. The objective of this department is to check the security of our customers’ digital assets and the data privacy aspect of their consumers and employees. The department also helps customers to verify if they have implemented security controls which are compliant to country laws, industry standards and other mandatory regulations.

Doris Brandl  
Data Protection Officer, TÜV SÜD Sec-IT GmbH  
Doris Brandl is a German lawyer and Data Protection Officer at TÜV SÜD Sec-IT GmbH in Munich. She has gained experience in the areas of Data Protection/Data Privacy Consulting Services (especially outsourcing, cloud computing, technical and organizational data security, drafting and negotiating data transfer and processing agreements) and Intellectual Property as well as auditing and implementing Compliance Management Systems with clients in Germany and Europe. She advises on all matters of data protection and is the external data protection officer of several companies.

Alexander Häußler  
Product Compliance Manager and Lead Auditor, TÜV SÜD Management Service  
Alexander Häußler is a Product Compliance Manager and a Lead Auditor for TÜV SÜD Management Service. Before joining TÜV SÜD, he was a software developer, systems administrator, and project leader responsible for introducing ISO 27001 at an automotive supplier. He then became the Information Security Officer at the same company. Currently he is supporting DIN and DAkkS in the workgroups dealing with ISMS topics.

Marcel Mangel  
Product Line Manager, Penetration Testing, TÜV SÜD Management Service  
Marcel Mangel is a computer scientist and is the Product Line Manager for Penetration Testing in TÜV SÜD Management Service in Munich. He has been working in the field of IT security for several years and has gained experience on both the offensive as well as defensive side. He also manages customer trainings as well as live hacking presentations.
Introduction

Cyberattacks against enterprise and industrial information technology (IT) systems are on the rise, with potentially costly consequences for companies, their customers and their executives. According to the international accounting firm PwC, the number of reported security incidents rose 48 percent in 2014 to nearly 43 million, an average of about 117,000 cyberattacks a day.¹ The number of reported incidents may be misleading, since it is estimated that 71 percent of cyberattacks go undetected.²

The potential threat of cyberattacks against so-called critical infrastructure industries has led governments around the world to implement regulations and requirements to help defend against such attacks or to minimize their impact. However, companies and businesses of all sizes are at risk. In fact, some cybersecurity consultants believe that small and midsized enterprises may actually be at greater risk since their IT infrastructures tend to be less secure and more susceptible to automated, large-scale attacks.³

Unfortunately, for many organizations, efforts to protect IT infrastructures tend to address the most likely nexus of cyberattacks, such as a company’s website or online payment system, or other potential vulnerabilities including system hardware. Yet, these approaches often fail to account for other areas of exposure that can be exploited by sophisticated hackers. In addition, most IT security implementations focus on solutions to historic vulnerabilities, while failing to account for hacker innovations. As a result, most IT security efforts fall short of providing a comprehensive, strategic approach that creates a more level playing field in the battle against hackers.
The growing IT security threat and its consequences

Today, IT systems are an indispensable component of economic activity throughout the industrialized world. Enterprises of all sizes depend on IT systems to process and store digitized data, including important documents and customer information. But IT systems also play a vital role in the control and monitoring of nearly every aspect of business operations, from manufacturing and industrial activities to point-of-sale transactions and web-based commerce. Therefore, in almost every modern organization, IT and other infrastructure systems are not just interrelated but are truly interdependent on each other. It is this thorough integration of IT systems in enterprise and industrial activities that significantly increases the potential for cyberattacks as well as the magnitude of the consequences. Security incidents that are detected have grown at a compounded annual growth rate of 66 percent year on year since 2009, a rate that shows no sign of abatement in the future. The annual global cost of cybercrime activities is estimated at more than $400 billion (USD), an amount greater than the gross domestic product of most countries.

Aside from the financial impact, organizations that are victimized by cyberattacks suffer other consequences. These include the loss of proprietary information that can weaken a company’s competitive position in the marketplace, a damaged reputation among current and prospective customers, and physical damages within the critical infrastructure industry. In some cases, senior executives have lost their jobs for failing to ensure the implementation of adequate IT security safeguards, or as a result of leaked communications that have compromised their integrity.

As the risk and consequences of cyberattacks increase, so too will spending on IT systems security. Information technology research and advisory firm Gartner, projects that expenditures will reach nearly $77 billion (USD) in 2015, an increase of 8.2 percent over expenditures in 2014. These and future increases will reportedly be driven by increased regulation and government oversight, as well as the introduction of new and more advanced
technologies that present a stronger defense against cyberattacks and other types of security breaches. Due to the increasing threat landscape, there is no 100% security. Therefore, the focus should remain on establishing an adequately high security level through security frameworks, with additional preventive and reactive services to minimize the response and countermeasure time when reacting against breaches.

The risks of cyberattacks are especially acute for industries and enterprises that have been identified as part of the critical infrastructure (CI), which is generally defined as “material and IT assets, networks, services and installations that, if disrupted or destroyed, would have a serious impact on the health, security or economic well-being of citizens and the efficient functioning of a country’s government.” More than 20 major industrialized countries or regions, including the U.S. and the European Union (EU), have designated CI-specific industry sectors, which typically include financial services, information technology, healthcare, telecommunication, utilities, energy, industrial transportation and aerospace and defense.

**HOLISTIC IT SECURITY STRATEGY**

<table>
<thead>
<tr>
<th>Preventive services</th>
<th>IT security framework</th>
<th>Reactive services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize digital risk</td>
<td>Meet relevant regulations</td>
<td>Reduce potential damages</td>
</tr>
</tbody>
</table>

**BENEFITS**

- Reduce response time
- Implement security control points
- Monitor security incidents
- Identify and secure sensitive data
- Country laws
- Supply chain requirements
- Industrial standards
- Speed up reaction time
- Identify data breaches
- Identify lost sensitive data
- Identify and close vulnerabilities

**SERVICES**

- Vulnerability checks
- Penetration testing
- IT security advisory services
- Data protection advisory services
- External data protection officer
- ISO/IEC 27001
- ISO 22301
- ISO/IEC 20000
- TL 9000
- PCI compliance
- s@fer shopping certification
- Data protection standards
- Certified Data Center
- Certified client data processing
- IT security forensics
- Breach response team
- …
IT security regulations

As IT security threats increase around the globe, so too do cyber security and data protection regulations and requirements. Most major jurisdictions have taken steps to implement IT security regulations applicable to both CI and non-CI industries. However, as illustrated in Figure 1, organizations operating in key CI-specific industries such as government, information technology and financials, are subject to a higher level of regulation and oversight since they face increased risks with potentially greater consequences.

In the EU, Council Directive 2008/114/EC, establishes a process for designating CI industry sectors in the EU, and a mechanism for assessing and reducing risk of cyberattacks in those sectors. Additional IT security requirements for organizations within designated CI industry sectors in the EU were expected to come into force in 2015 with the approval of the EU’s Network and Information Security (NIS) Directive.16 Organizations in both CI and non-CI industries are also currently subject to stringent data protection regulations regarding the protection of any personal data of individuals they may collect, process or retain. Under the essential requirements of the EU’s Data Protection Directive 95/46/EC, organizations that collect or manage personal information must “implement appropriate technical and organizational measures to protect
personal data against… unauthorized disclosure or access.” The provisions of the EU’s Data Protection Directive are slated to be replaced in early 2016 with a new General Data Protection Regulation (GDPR), which is expected to address technological developments that have impacted data protection efforts since the implementation of the original Data Protection Directive nearly 20 years ago.

Individual EU member states, including Germany, Poland, the United Kingdom and Italy have implemented or are in the process of implementing country-specific cybersecurity regulations applicable to organizations in CI industry sectors. In Germany, for example, the IT Security Act (ITSiG) was passed in June 2015. The legislation requires companies to implement adequate organizational and technical measures to protect IT systems.

In the U.S., a greater awareness of the dangers posed by cybersecurity threats has resulted in a host of industry-specific regulations and standards, such as data protection standards applicable in the U.S. healthcare industry. Nonetheless, Presidential Executive Order 13636, issued in February 2013, establishes a holistic approach to IT security that relies on voluntary adoption of effective cybersecurity practices, facilitating the sharing of cyber threat information, and exploring the use of existing regulations to promote cyber security. The Executive Order also called for the development of a voluntary risk-based Cybersecurity Framework, which was published in February 2014 by the U.S. National Institute of Standards and Technology (NIST). The Cybersecurity Framework is designed to help organizations view cybersecurity risks and mitigation activities in the context of their overall risk management assessment and management efforts.
In general, the extent of regulatory requirements affecting enterprises in individual countries depends on the degree of the perceived threat in that country. This relationship is illustrated in Figure 2, which is based on extensive research by TÜV SÜD, and scores on the Y-axis, the current and proposed cybersecurity and data protection laws of countries in a 60% and 40% weightage.

However, most cybersecurity regulatory schemes and frameworks applicable to CI sector enterprises strive to increase the security of IT systems through a combination of regulations and voluntary cooperative efforts between government and the private sectors, such as security breach notification and information sharing initiatives. Many individual jurisdiction schemes also promote a broader reliance on IT security standards, such as ISO 27001, the international standard for information security management.
The changing regulatory landscape is being driven in large part by a significant increase in the number and sophistication of persistent threats. One example of this trend is the advanced persistent threat (APT), a set of stealthy and continuous computer hacking processes often targeting a specific entity. Specifically, the “advanced” threat signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The “persistent” process suggests that an external command and control system is continuously monitoring and extracting data from a specific target.

The term APT is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information. It also applies equally to other types of threats, such as traditional espionage or organized criminal activity.

In combination with the various types of cyber threats, the likelihood of a successful cyberattack depends on the extent to which an individual IT system is vulnerable to such threats. System vulnerabilities take a number of different forms, depending on the scope of the IT system and the degree of integration with other industrial systems and infrastructure operations. Other vulnerability factors include:

### Types of IT security threats and vulnerabilities

- **Increased Connectivity**: The integration of IT systems with other networks and operating controls increases the flow of information but eliminates the physical isolation that helps to protect those systems against outside threats.

- **Off-the-Shelf Components**: Increasingly, IT systems are designed from off-the-shelf components, which reduces costs and implementation time. But outside knowledge of component security vulnerabilities is more likely to be available.

- **Wireless Connectivity**: Today’s IT systems support wireless connections to ease data collection from off-site locations. However, wireless connectivity is more vulnerable to eavesdropping and remote hacking activities.

- **Fewer Security Features**: In addition to the above security vulnerabilities, the design of other IT systems elements, such as underlying embedded devices and application software, may compromise overall IT security.

- **Vendor Access and Security Requirements**: Lastly, outside vendors with direct access to an organization’s IT system may have less stringent IT security measures in place, thereby providing an alternate path for hackers and cyberattacks.

---

**IT SYSTEM VULNERABILITY FACTORS**

System vulnerabilities take a number of different forms, depending on the scope of the IT system and the degree of integration with other industrial systems and infrastructure operations. The graphic below illustrates 5 other vulnerability factors.
Elements for broader approach to IT security

Until recently, the majority of IT security efforts have focused on programs and controls specifically intended to address IT infrastructure. These efforts usually include the development and application of specific technical requirements for IT hardware and components, the effectiveness of which can be assessed through focused testing such as hardware penetration testing. Depending on their business or the nature of their operations, some organizations may also rely on supervisory control and data acquisition (SCADA) systems for specific operational activities, or take other approaches to security that follow industry accepted standards and practices.

As previously noted, the integration of IT systems with other infrastructure elements can introduce unforeseen vulnerabilities that put at risk not just core IT systems but business assets throughout the organization. In this dynamic threat environment, these vulnerabilities render the standard, manpower-intensive approach to IT security insufficient to address the modern cyber threat landscape.

What’s required instead is a broader approach to IT security that isn’t defined only by security within specific operations, but which establishes an IT security framework at the enterprise-wide level. At a minimum, this framework would include:

- Organization-wide policies and procedures to identify and secure sensitive data
- Analytic and intelligence gathering capabilities to assess general threat levels and areas of vulnerability
- Intelligent software platforms expressly designed to detect and evaluate relevant security threats, and to determine the appropriate response to an identified security breach
- Audits to ensure compliance with country and industrial IT security regulations and standards
- Risk analysis
- Efficient and accurate implementation of needed IT security software

Once an organization’s IT security framework has been established, routine preventative activities could include system vulnerability checks and penetration testing analysis of incidents. Ongoing activities could also include system compliance monitoring as well as forensic investigations following actual security breaches to identify root causes.

In taking this more holistic approach to IT security, organizations can immediately achieve important gains in their efforts to defend against cyberattacks, regardless of their source or type. In addition, it facilitates the integration of IT security efforts into enterprise-wide risk management programs, transforming IT security into a critical aspect of an organization’s overall business strategy.
Step towards an effective IT security strategy

The successful implementation of a more effective IT security program can benefit from taking a structured approach that includes the following steps:

1. **Gain senior management commitment**
   - Success starts with clear and unequivocal commitment from an organization’s senior management to IT security and to the implementation of a program that meets the needs of the organization.

2. **Align IT security efforts with business objectives**
   - To gain widespread employee compliance with IT security policies, initiatives must be seen as directly supporting the key business objectives and activities of the organization.

3. **Implement an IT security management system**
   - ISO 27001 provides a valuable framework for the development and implementation of an information security management system, while providing the flexibility necessary to accommodate specific requirements.

4. **Pre-evaluate security issues associated with new technologies**
   - The introduction of new technologies also brings the potential for new system vulnerabilities. Security concerns should be vetted and evaluated prior to the introduction of any new technology that could affect the overall security of the IT system.

5. **Foster awareness and accountability of IT security issues throughout the organization**
   - The steady flow of information regarding IT security will help to ensure management and employee engagement with IT security principles and practices. Incorporating security considerations into an organization’s performance management process can drive accountability at all levels.

6. **Leverage industry knowledge and expertise**
   - No single organization has all of the answers when it comes to IT security. Accessing the expertise available through industry and trade associations and cybersecurity specialists can reduce the time needed to implement effective security solutions as well as the risk from cyber threats.
As cyberattacks become commonplace, the need for an effective approach to IT security becomes even more critical. However, many organizations, including those that are part of the critical infrastructure, are moving slowly to address today’s cyber threats. What’s more, many IT security approaches fail to account for vulnerabilities resulting from the integration of IT systems with other data-driven operations, making them even more susceptible to attack with all of the attendant consequences.

To successfully address these challenges, organizations must consider adopting a broader approach to IT security, one that accounts for enterprise-wide risks and vulnerabilities, complements other risk management practices, and elevates IT security to a strategic priority. This holistic approach offers greater security against today’s threats, and better positions organizations to address unknown cyber challenges in the future.

TÜV SÜD is a global provider of a complete range of enterprise and industrial IT security services and solutions. Our service portfolio includes data security services, such as IT penetration testing, data protection audits, and payment card industry compliance testing for those organizations that handle credit card data. TÜV SÜD’s own S@fer-Shopping Mark for e-commerce is widely recognized as evidence of a website that has been thoroughly evaluated for maintaining the security of consumer information. TÜV SÜD is also a leading registrar for ISO/IEC 27001, ISO 22301 (business continuity management), and TL 9000 (quality management requirements for the telecom industry). These credentials make TÜV SÜD the IT security partner of choice for CI sector organizations and enterprises large and small around the world.
GLOSSARY OF ACRONYMS

APT — advanced persistent threat
CI — critical infrastructure
EU — european union
GDPR — general data protection regulation
IT — information technology
NIS — network and information security
NIST — national institute of standards and technology
SCADA — supervisory control and data acquisition

FOOTNOTES


COPYRIGHT NOTICE

The information contained in this document represents the current view of TÜV SÜD on the issues discussed as of the date of publication. Because TÜV SÜD must respond to changing market conditions, it should not be interpreted to be a commitment on the part of TÜV SÜD, and TÜV SÜD cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. TÜV SÜD makes no warranties, express, implied or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of TÜV SÜD.

DISCLAIMER

All reasonable measures have been taken to ensure the quality, reliability, and accuracy of the information in the content. However, TÜV SÜD is not responsible for the third-party content contained in this newsletter. TÜV SÜD makes no warranties or representations, expressed or implied, as to the accuracy or completeness of information contained in this newsletter. This newsletter is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). Accordingly, the information in this newsletter is not intended to constitute consulting or professional advice or services. If you are seeking advice on any matters relating to information in this newsletter, you should — where appropriate — contact us directly with your specific query or seek advice from qualified professional people. The information contained in this newsletter may not be copied, quoted, or referred to in any other publication or materials without the prior written consent of TÜV SÜD. All rights reserved © 2016 TÜV SÜD.
Reduce potential damage with a holistic IT security approach

Choose certainty. Add value.
TÜV SÜD is a premium quality, safety, and sustainability solutions provider specializing in testing, inspection, auditing, certification, training, and knowledge services. Represented by more than 22,000 employees across 800 locations worldwide, TÜV SÜD’s service portfolio adds value to businesses, consumers and the environment.